UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/813,346 | 03/29/2004 | Osamu Kobayashi | GENSP151C1 | 5003 |

22434 7590 02/15/2006

BEYER WEAVER & THOMAS LLP
P.O. BOX 70250
OAKLAND, CA 94612-0250

| EXAMINER | |
|---|---|
| SHERKAT, AREZOO | |
| **ART UNIT** | **PAPER NUMBER** |
| 2131 | |

DATE MAILED: 02/15/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/813,346 | KOBAYASHI ET AL. | |
| | Examiner | Art Unit | |
| | Arezoo Sherkat | 2131 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *27 December 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1 and 4-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1 and 4-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *29 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

### *Response to Amendment*

This office action is responsive to Applicant's amendment received on December 27, 2005. Claims 2-3 are cancelled. Claims 1, 4, 6, and 12 are amended. Claims 1 and 4-22 are pending.

### *Response to Arguments*

Applicant's arguments with respect to claims 1 and 4-22 have been considered but are moot in view of the new ground(s) of rejection.

### *Claim Rejections - 35 USC § 103*

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1 and 4-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over High-bandwidth Digital Content Protection System, Revision 1.0 by Intel Corporation and HDCP Revision 1.0 hereinafter), in view of Matyas et al., (U.S. Patent No. 5,142,578 and Matyas hereinafter).

Regarding claims 1, 4-5, and 12-16, HDCP Revision 1.0 discloses a method of using a cryptographic key in a display device, comprising:

in a display device having a printed circuit board (PCB) and a master block, providing a key to the PCB by the master block (HDCP Revision 1.0, Pages 6-27).

HDCP Revision 1.0 does not expressly disclose encrypting the cryptographic keys before storing them.

However, Matyas discloses selecting one of a number of available encryption protocols for each of the provided keys (i.e., such as authentication key), encrypting each of the provided keys based upon a particular one of the selected encryption protocols, storing the encrypted keys in a non-volatile memory by the PCB, decrypting the stored encrypted key, as needed, by the PCB based upon the selected encryption protocol (i.e., KMb.C6 is formed as the exclusive or product of the master key, KMb, stored in CF 30' and control vector C6. Thus the type and usage attributes assigned by the originator of the key-encrypting key in the form of a control vector are cryptographically coupled to the key-encrypting key such that the recipient may only use the received key-encrypting key in a manner defined by key generatore)(Col. 9, lines 57-67 and Col. 10-11, lines 1-67 and Col. 12, lines 1-27).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of HDCP Rvision 1.0 with teachings of Matyas because it would allow to include securely recovering the distributed key-encrypting key by the recipient by decrypting the received key record using the same public key algorithm and private key associated with the public key and renecrypting the key-encrypting key under a key formed by arithmetically combining the recipient's master key with a control vector contained in the control information of the received key

recored as disclosed by Matyas. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Matyas to provide more security in a cryptographic system implementing both a symmetric encryption algorithm such as a Data Encryption Standard and an asymmetric encryption algorithm such as RSA public key algorithm (Matyas, Col. 4, lines 50-67 and Col. 5, lines 1-20).

Regarding claims 6-9, 11, 17-20, and 22, HDCP Revision 1.0 discloses wherein the plurality of keys includes a decryption key and an authentication key (i.e., HDCP authentication protocol and HDCP cipher)(HDCP Revision 1.0, Pages 6).

Regarding claims 10 and 21, HDCP Revision 1.0 does not expressly disclose encrypting the cryptographic keys.

However, Matyas discloses retrieving an encrypted authentication key (i.e., public and private keys) from the non-volatile memory corresponding to the authentication request, and decrypting the authentication request based upon a corresponding decryption protocol (i.e., the exclusive or product of master key and the control vector)(Col. 7, lines 54-67 and Col. 8, lines 1-14).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of HDCP Rvision 1.0 with teachings of Matyas because it would allow to include securely recovering the distributed key-encrypting key by the recipient by decrypting the received key record using the same

public key algorithm and private key associated with the public key and renecrypting the key-encrypting key under a key formed by arithmetically combining the recipient's master key with a control vector contained in the control information of the received key recored as disclosed by Matyas. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Matyas to provide more security in a cryptographic system implementing both a symmetric encryption algorithm such as a Data Encryption Standard and an asymmetric encryption algorithm such as RSA public key algorithm (Matyas, Col. 4, lines 50-67 and Col. 5, lines 1-20).

***Conclusion***

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Arezoo Sherkat whose telephone number is (571) 272-3796. The examiner can normally be reached on 8:00-4:30 Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

A. Sherkat

Arezoo Sherkat
Patent Examiner
Group 2131
Feb. 7, 2006

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100